

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. - 6. (Canceled)

7. (Currently Amended) A key recovery system comprising:
an encryption apparatus using key information for encrypting or decrypting data and storing, independently of the key information, recovery information for recovering the key information in an encrypted state so as to be decrypted by a key recovery agent registered by said encryption apparatus;
an approver apparatus for approving a party who requests a registration approval for the key recovery agent and giving an authorized party who requests an approval for decrypting the encrypted recovery information the approval for decrypting the encrypted recovery information; and
said ~~decrypter apparatus~~ key recovery agent for decrypting and sending the encrypted recovery information only when a decryption request is made by a party approved by an approver.

8. (Canceled)

9. (New) A cryptographic communication system comprising:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

an encryption apparatus for encrypting a data body and for transmitting transmission data to a receiver, the transmission data including:

an encrypted data body;

sender's key recovery data obtained by encrypting recovery information for recovering a key for decrypting the encrypted data body to allow a key recovery agent registered by a sender to decrypt the recovery information; and

receiver's key recovery data obtained by encrypting the recovery information for recovering the key for decrypting the encrypted data body to allow the key recovery agent registered by the receiver to decrypt the recovery information;

a plurality of the key recovery agents each, when registered by the sender or the receiver, capable of decrypting a sender's or a receiver's key comprised of a plurality of key pieces obtained by dividing the key into pieces, wherein each key recovery agent decrypts and sends back the sender's or the receiver's key recovery data only when a request is made by a party approved by an approver; and

an approver apparatus for approving a requester for a key recovery agent registration approval and approving an authorized third party, who requests an approval for decrypting the sender's or the receiver's key recovery data, to decrypt the sender's or the receiver's key recovery data.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

10. (New) A cryptographic communication system comprising:

an encryption apparatus for encrypting a data body and for transmitting transmission data to a receiver, the transmission data including:

an encrypted data body;

sender's key recovery data obtained by encrypting recovery information for recovering a key for decrypting the encrypted data body to allow a key recovery agent registered by a sender to decrypt the recovery information; and

receiver's key recovery data obtained by encrypting the recovery information for recovering the key for decrypting the encrypted data body to allow the key recovery agent registered by the receiver to decrypt the recovery information;

a plurality of the key recovery agents each, when registered by the sender or the receiver, capable of decrypting a sender's or a receiver's key comprised of a plurality of key pieces obtained by dividing the key into pieces, wherein each key recovery agent decrypts and sends back the sender's or the receiver's key recovery data only when a request is made by a party approved by an approver;

a certificate authority apparatus arranged to allow accepting registration of at least the key recovery agent and receivers and provide information representing correspondence between each registered receiver and the key

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

recovery agent and information representing that said encryption apparatus encrypts the recovery information so as to allow the key recovery agent to decrypt the recovery information; and

an approver apparatus for approving a requester for a key recovery agent registration approval and approving an authorized third party, who requests an approval for decrypting the sender's or the receiver's key recovery data, to decrypt the sender's or the receiver's key recovery data.

11. (New) A key recovery method comprising:

using key information for encrypting or decrypting data and storing, independently of the key information, recovery information for recovered key information in an encrypted state so as to be decrypted by a key recovery agent registered by an encryption apparatus;

approving a party who requests a registration approval for the key recovery agent and giving an authorized party who requests an approval for decrypting an encrypted recovery information, the approval for decrypting the encrypted recovery information; and

decrypting and sending the encrypted recovery information only when a decryption request is made by a party approved by an approver.

12. (New) A cryptographic communication method comprising:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

encrypting a data body;

transmitting transmission data to a receiver, the transmission data
including:

an encrypted data body;

sender's key recovery data obtained by encrypting recovery
information for recovering a key for decrypting the encrypted data body to allow a
key recovery agent registered by a sender to decrypt the recovery information;
and

receiver's key recovery data obtained by encrypting the recovery
information for recovering the key for decrypting the encrypted data body to allow
the key recovery agent registered by the receiver to decrypt the recovery
information; and

decrypting, by each of a plurality of key recovery agents, when registered
by the sender or the receiver, a sender's or a receiver's key comprised of a
plurality of key pieces obtained by dividing the key into pieces; and

approving, by an approving apparatus, a requester for a key recovery
agent registration approval and approving an authorized third party, who
requests an approval for decrypting the sender's or the receiver's key recovery
data, to decrypt the sender's or the receiver's key recovery data wherein the
sender's or the receiver's key recovery data sent only when a request is made by
a party approved by an approver.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

13. (New) A cryptographic communication method, comprising:

encrypting a data body;

transmitting transmission data to a receiver, the transmission data

including:

an encrypted data body;

sender's key recovery data obtained by encrypting recovery

information for recovering a key for decrypting the encrypted data body to allow a

key recovery agent registered by a sender to decrypt the recovery information;

and

receiver's key recovery data obtained by encrypting the recovery

information for recovering the key for decrypting the encrypted data body to allow

the key recovery agent registered by the receiver to decrypt the recovery

information;

decrypting, by each of a plurality of the key recovery agents, when
registered by the sender or the receiver, a sender's or a receiver's key comprised
of a plurality of key pieces obtained by dividing the key into pieces;

accepting a registration of at least the key recovery agent and receivers
and providing information representing correspondence between each registered
receiver and the key recovery agent and information representing that said
encryption apparatus encrypts the recovery information so as to allow the key
recovery agent to decrypt the recovery information;

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

approving a requester for a key recovery agent registration approval and approving an authorized third party, who requests an approval for decrypting the sender's or the receivers key recovery data, to decrypt the sender's or the receiver's key recovery data; and

said decrypting and sending the sender's or receiver's key recovery data is made only when a request is made by a party approved by an approver.

14. (New) An article of manufacture comprising:

a computer usable medium having computer readable program code means embodied therein for recovery of a key, the computer readable program code means further comprising:

means for causing a computer to use key information for encrypting or decrypting data and storing, independently of the key information, recovery information for recovering the key information in an encrypted state so as to be decrypted by a key recovery agent registered by an encryption apparatus;

means for causing the computer to approve a party who requests a registration approval for the key recovery agent and giving an authorized party who requests an approval for decrypting the encrypted recovery information the approval for decrypting the encrypted recovery information; and

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

means for causing the computer to decrypt and send the encrypted recovery information only when a decryption request is made by a party approved by an approver.

15. (New) An article of manufacture comprising:

a computer usable medium having computer readable program code means embodied therein for facilitating a cryptographic communication method, the computer readable program code means further comprising:

means for causing a computer to encrypt a data body;

means for causing the computer to transmit transmission data to a receiver, the transmission data including:

an encrypted data body;

sender's key recovery data obtained by encrypting recovery information for recovering a key for decrypting the encrypted data body to allow a key recovery agent registered by a sender to decrypt the recovery information; and

receiver's key recovery data obtained by encrypting the recovery information for recovering the key for decrypting the encrypted data body to allow a key recovery agent registered by a receiver to decrypt the recovery information; and

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

means for causing the computer to decrypt, by each of a plurality of key recovery agents, when registered by a sender or a receiver, senders or receivers key comprised of a plurality of key pieces obtained by dividing the key into pieces;

means for causing the computer to approve, by an approving apparatus, a requester for a key recovery agent registration approval and approving an authorized third party, who requests an approval for decrypting the sender's or the receiver's key recovery data, to decrypt the sender's or the receiver's key recovery data, and

means for causing the computer to decrypt and send the sender's or the receiver's key recovery data only when a request is made by a party approved by an approver.

16. (New) An article of manufacture comprising:

a computer usable medium having computer readable program code means embodied therein for facilitating a cryptographic communication method, the computer readable program code means further comprising:

means for causing a computer to encrypt a data body;

means for causing the computer to transmit transmission data to a receiver, the transmission data including:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

means for causing the computer to include into the transmission
data:

an encrypted data body;

sender's key recovery data obtained by encrypting recovery
information for recovering a key for decrypting an encrypted data body to allow a
key recovery agent registered by a sender to decrypt the recovery information;
and


receiver's key recovery data obtained by encrypting the recovery
information for recovering the key for decrypting the encrypted data body to allow
the key recovery agent registered by a receiver to decrypt the recovery
information; and

means for causing the computer to decrypt, by each of a plurality of key
recovery agents, when registered by sender or receiver, senders or receivers key
comprised of a plurality of key pieces obtained by dividing the key into pieces;

means for causing the computer to accept a registration of at least the key
recovery agent and receivers and provide information representing
correspondence between each registered receiver and the key recovery agent
and information representing that said encryption apparatus encrypts the
recovery information so as to allow the key recovery agent to decrypt the
recovery information;

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

 means for causing the computer to approve a requester for the key recovery agent registration approval and approving an authorized third party, who requests an approval for decrypting the sender's or the receiver's key recovery data, to decrypt the sender's or the receiver's key recovery data; and

means for causing the computer to decrypt and send back the sender's or the receiver's key recovery data only when a request is made by a party approved by an approver.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com